BOBBY JINDAL
GOVERNOR

ANGELE DAVIS
COMMISSIONER OF ADMINISTRATION

State of Louisiana

Division of Administration
Office of Information Technology

MONTHLY SECURITY TIPS November 2008

Use Caution with USB Drives

Overview

USB drives are popular for storing and transporting data, but some of the characteristics that make them convenient also introduce security risks.

What security risks are associated with USB drives?

Because USB drives, sometimes known as thumb drives, are small, readily available, inexpensive, and extremely portable, they are popular for storing and transporting files from one computer to another. However, these same characteristics make them appealing to attackers.

One option is for attackers to use your USB drive to infect other computers. An attacker might infect a computer with malicious code, or malware, that can detect when a USB drive is plugged into a computer. The malware then downloads malicious code onto the drive. When the USB drive is plugged into another computer, the malware infects that computer.

Some attackers have also targeted electronic devices directly, infecting items such as electronic picture frames and USB drives during production. When users buy the infected products and plug them into their computers, malware is installed on their computers.

Attackers may also use their USB drives to steal information directly from a computer. If an attacker can physically access a computer, he or she can download sensitive information directly onto a USB drive. Even computers that have been turned off may be vulnerable, because a computer's memory is still active for several minutes without power. If an attacker can plug a USB drive into the computer during that time, he or she can quickly reboot the system from the USB drive and copy the computer's memory, including passwords, encryption keys, and other sensitive data, onto the drive. Victims may not even realize that their computers were attacked.

The most obvious security risk for USB drives, though, is that they are easily lost or stolen. If the data was not backed up, the loss of a USB drive can mean hours of lost work and the potential that the information cannot be replicated. And if the information on the drive is not encrypted, anyone who has the USB drive can access all of the data on it.

Recommendations

To help mitigate the risks of using Removable Media Devices, we recommend the following:

- Take advantage of security features - Use passwords and encryption on your USB drive to protect the data, and ensure the information on the drive is backed up in case it is lost.
- Lock USB ports or control the use of USB ports using configuration control software.
- Keep personal and business thumb drives separate - Do not use personal USB drives on computers owned by your organization, and do not plug USB drives containing corporate information into your personal computer.
- Keep systems up-to-date with the latest patches and anti-virus signatures.
- Do not plug an unknown USB drive into a computer - If a USB drive is found, give it to the appropriate authorities (a location's security personnel, your organization's IT department, etc.). Do not plug it into a computer to view the contents or to try to identify the owner.

The information provided in this Monthly Security Tips Newsletter is intended to increase the security awareness of end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the State's overall cyber security posture.

The above information was obtained from the **US-CERT**, a component of the **U.S. Department of Homeland Security**.